Your quality partner for software solutions

Information Security Awareness Training

Security Department

Nov 2020

ISO9001 Version 2015

ISO27001 Version 2013

CMMI Level 5

TL9000

Microsoft Partner
Gold Software Development
Gold Data Platform

Contents

- What and Why Information Security?
- ISMS Introduction
- Responsibilities
- Policies and Best Practices
- Safety Procedures
- General Data Protection Regulation
- Security Audit
- NDA Compliance

Contents

- **What and Why Information Security?**
- ISMS Introduction
- Responsibilities
- Policies and Best Practices
- Safety Procedures
- General Data Protection Regulation
- Security Audit
- NDA Compliance

What is information?

Information is an asset, like other important business assets, has value to an organization and consequently needs to be suitably protected

- Printed or written on paper
- Stored electronically
- Displayed or published on web
- Verbal – spoken in conversations
- Transmitted by post or using electronic
- Corrupted
- Lost
- Stolen

What is information security?

For protecting information and information system from:

Unauthorized access, use, disclosure, disruption, modification, or destruction

- **Confidentiality**

Ensuring that information is accessible only to those authorized to have access

- **Integrity**

Safeguarding the accuracy and completeness of information and processing methods

- **Availability**

Ensuring that authorized users have access to information and associated assets when required

Why information security?

- Protect information ASSETS from a range of THREATS
- Brand and reputation
- Minimize financial loss
- Optimize return on investments
- Increase business opportunities
- Competitive advantage
- Enable business continuity and disaster recovery

Assets

- **Papers**
  - Contracts, HR records
- **Digital information**
  - Databases, files, documents
- **Hardware**
  - Computers, devices, equipments, supporting utilities
- **Software**
  - Operating systems, applications, development tools
- **Services**
  - Email, web, internet, telecommunications
- **People**
  - Employees, customers, contractors

Threats

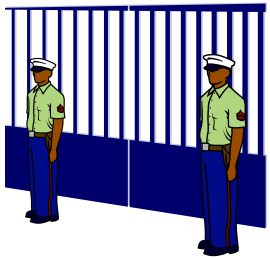
High User Knowledge of IT Systems

Theft, Sabotage, Misuse

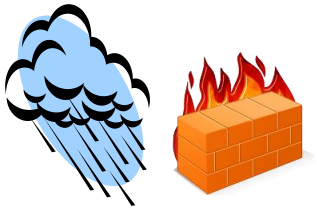
Virus Attacks

Systems & Network Failure

Lack Of Documentation

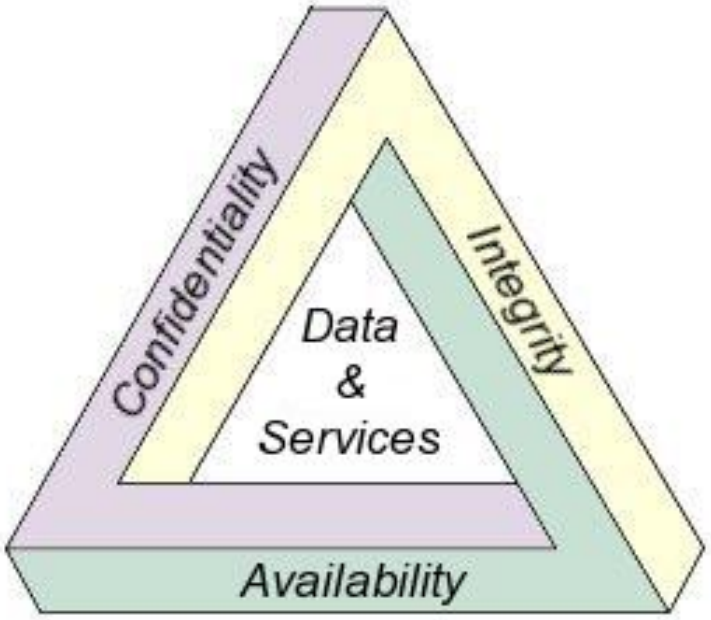


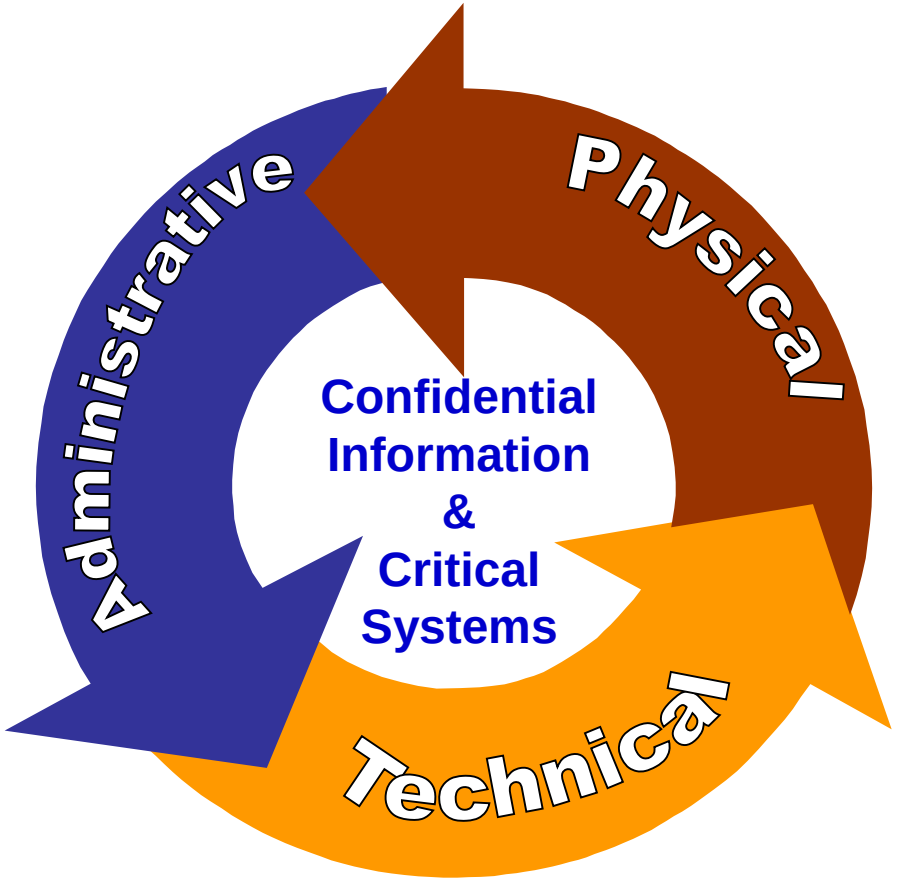
Lapse in Physical Security



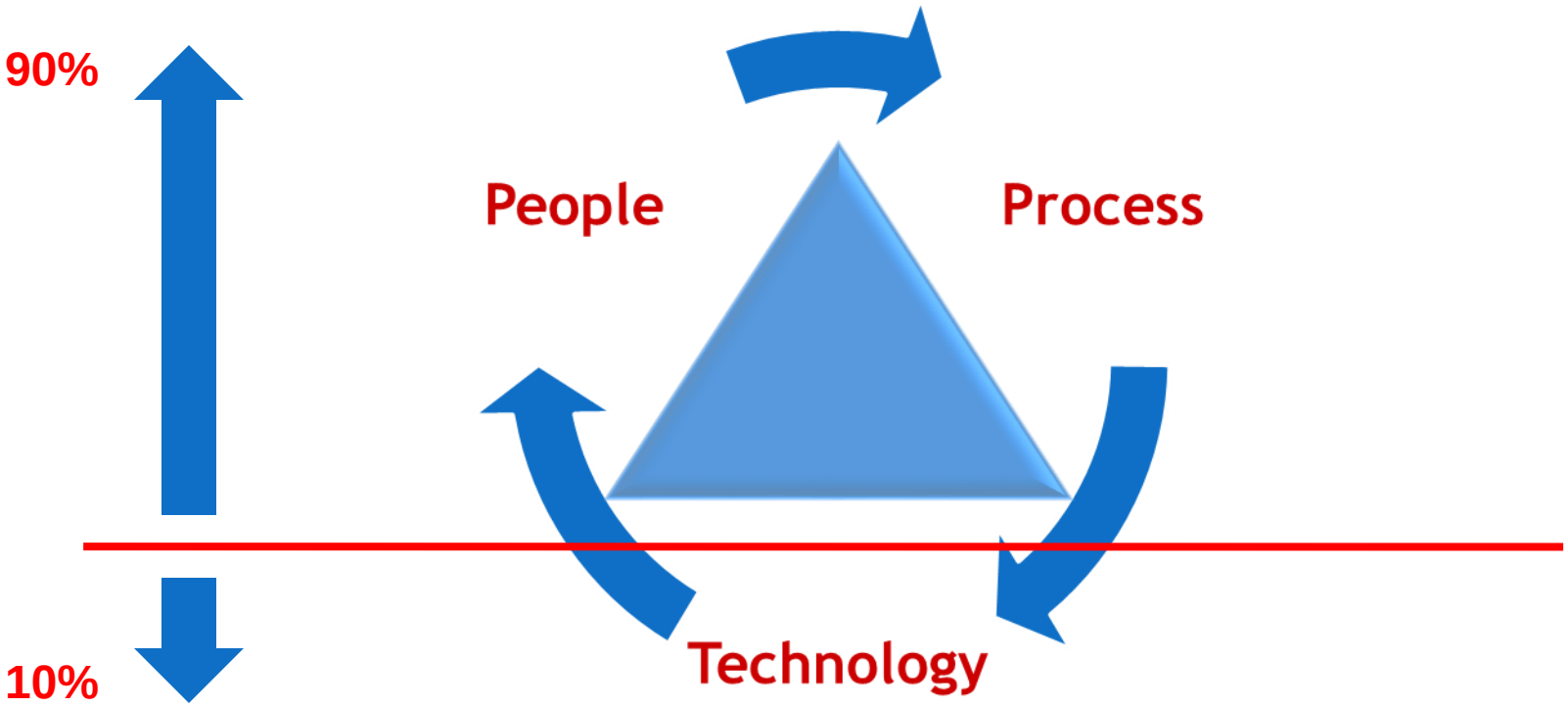
Natural Disasters & Fire

Information security goal





Security system



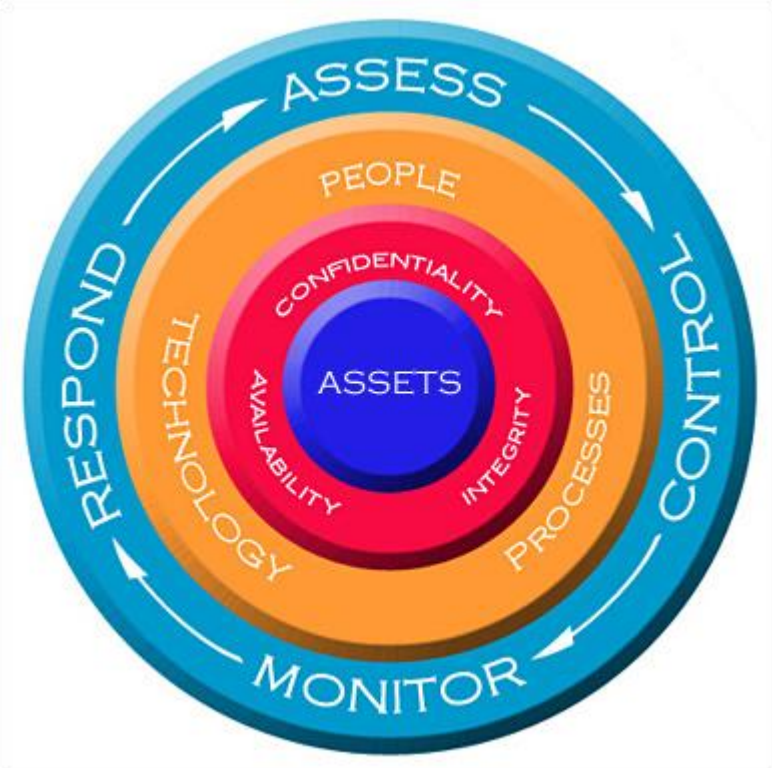
Security is Everyone's responsibility!

Contents

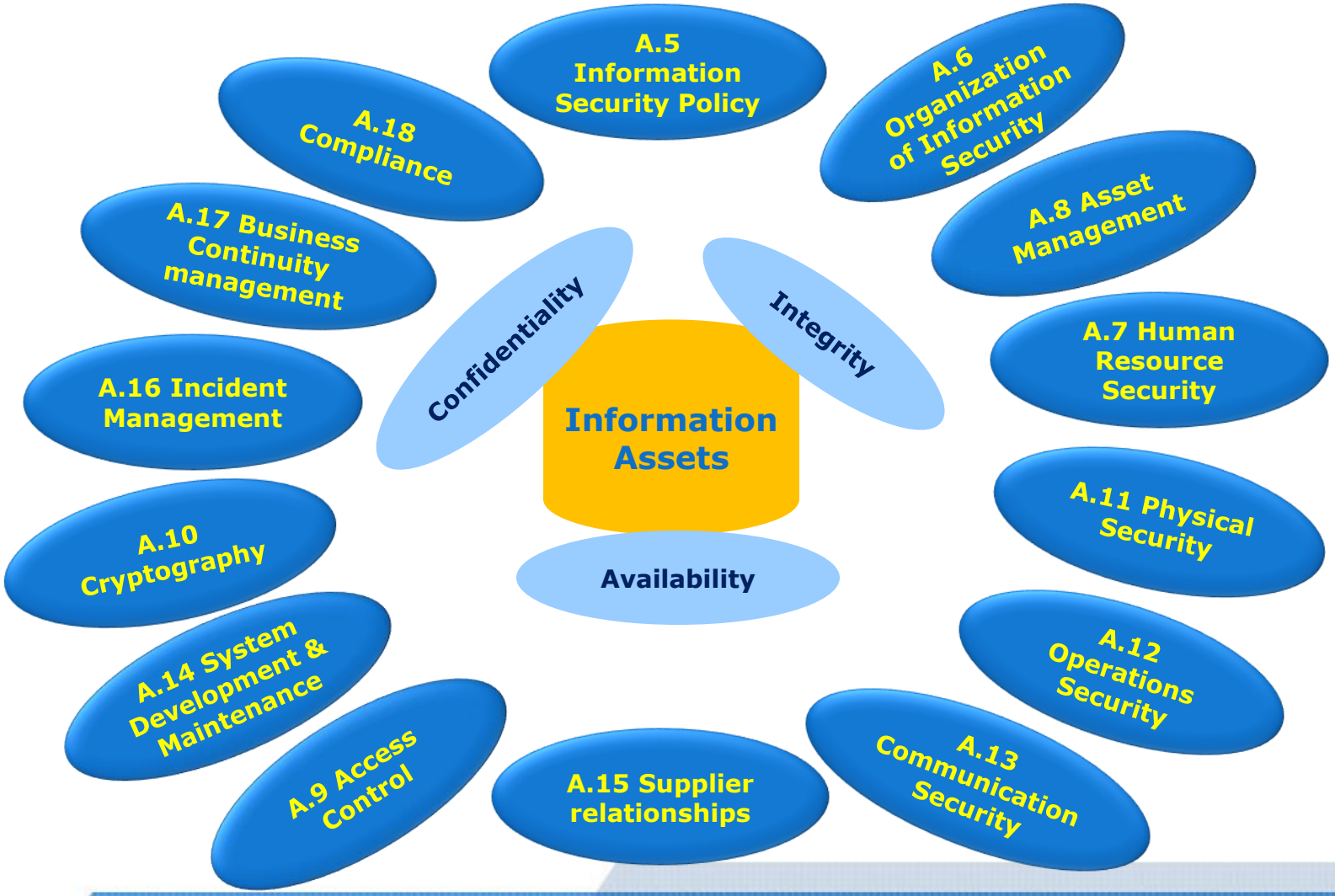
- What and Why Information Security?
- **ISMS Introduction**
- Responsibilities
- Policies and Best Practices
- Safety Procedures
- General Data Protection Regulation
- Security Audit
- NDA Compliance

Information Security Management System

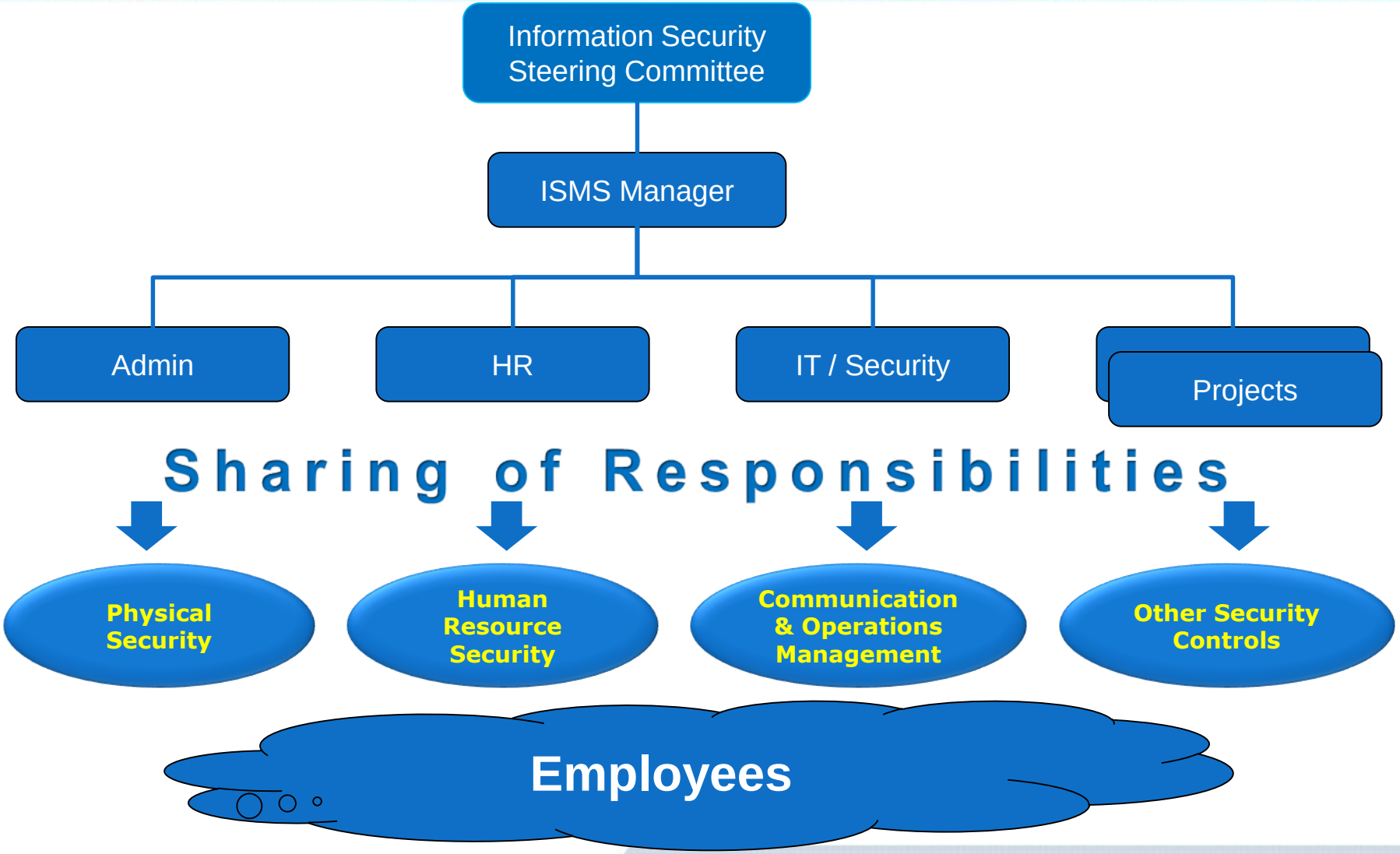
- http://intranet.tma.com.vn/qms/ISMS.htm



Security controls



Security organization



Contents

- What and Why Information Security?
- ISMS Introduction
- **Responsibilities**
- Policies and Best Practices
- Safety Procedures
- General Data Protection Regulation
- Security Audit
- NDA Compliance

Responsibilities: Manager/Security Prime

- Ensure team members follow security policies and procedures(Exp: GDPR)
- Report incidents/violations to Security Team timely
- Work with other Security Team members to solve security issues in the project
- Is available to answer security concerns from other team members
- Regularly perform security review, risk assessment for the project (e.g access rights on SVN, local server, GIT, project profile, keywords…)

Responsibilities: Employee

- Follow the policies, procedures, standards, regulations… defined in company
- Commit to protect TMA and customers' Intellectual Property and confidential information
- Apply security best practices to daily activities
- Timely report security incidents, violations or misuses
- Contribute ideas to make security better

SEC- U - R - IT -Y

Contents

- What and Why Information Security?
- ISMS Introduction
- Responsibilities
- **Policies and Best Practices**
- Safety Procedures
- General Data Protection Regulation
- Security Audit
- NDA Compliance

Information Security Policies

POLICIES

- ISMS-PO-001-Information Security Policy
- ISMS-PO-002-Compliance Policy
- ISMS-PO-003-Information Systems Acquisition Development and Maintenance Policy
- ISMS-PO-004-Access Control Policy
- ISMS-PO-005-Information Security Incident Management Policy
- ISMS-PO-006-Business Continuity Management Policy
- ISMS-PO-007-Physical And Environmental Security Policy
- ISMS-PO-008-Asset Management Policy
- ISMS-PO-009-Acceptable Use Policy
- ISMS-PO-011- Operations Management Policy
- ISMS-PO-012-Human Resources Policy
- ISMS-PO-013-Antivirus Policy
- ISMS-PO-014-Network Usage Policy
- ISMS-PO-015-Mobile Mail Policy
- ISMS-PO-016-Wireless Policy
- ISMS-PO-017-Teleworking Policy
- ISMS-PO-018-Email Policy
- ISMS-PO-019-File Sharing Service Policy
- ISMS-PO-020-SVN Policy
- ISMS-PO-021-Privileged Internet Access Policy
- ISMS-PO-022-Telecom Policy
- ISMS-PO-023-Change And Problem Management Policy
- ISMS-PO-024-Backup Restore Policy
- ISMS-PO-025-Cryptography Policy
- ISMS-PO-027-Communications Security Policy
- ISMS-PO-028-Secure Development Policy
- ISMS-PO-029-Supplier Relationships Policy
- ISMS-PO-030-General Data Privacy Policy

PROCESSES

- ISMS-PC-001-Information Security Risk Management Process
- CO-PC-005-Internal Audit Process
- CO-PC-008-Nonconformity Handling Process
- CO-PC-002-Records Control Process
- CO-PC-001-Documents Control Process

PROCEDURES

- ISMS-PR-001-ISMS Management Review procedure
- IS-PR-009-New Desktop Setup Procedure
- CO-PR-016-Department Measurement and Analysis Procedure
- IT System Procedures
- Security Procedures
- Human Resource Procedures
- Admin Procedures

Acceptable Uses

- Data created on the corporate systems remains the property of TMA
- TMA equipments, services are for business purpose only
- Using unauthorized storage devices (USB, HDD, CD/DVD, …), computing facilities (laptop, PC, …) inside TMA premises **is not permitted**
- Users are responsible for securing assigned equipments following defined guidelines and accountable for any misuses, violations found
- Food, drink in lab room, network and storage room is not permitted.

IP & Confidential information protection

- Fully aware of importance of protecting and using Intellectual Property and confidential information
- Understand TMA's information classification
  - Public, Confidential, Critical Confidential
- Always encrypt confidential information when transfer, bring to outside
- Report any misuse of company data

- Gossip about confidential information
- Post confidential information to social network websites (Facebook, Linkedin, etc)
- Upload/Email/Post confidential information to internet
- Bring confidential information outside without prior approval

Cloud Best Practices(1)

- **Protect account access with two-factor authentication**
- **Account management**
  - KEY(AKxxxx) should storage at local configuration file
  - Never commit secrets ”KEY” into GIT repos
  - Sharing only with authorized personnel, tight management
- **Access control/monitor for staff via KEY**
  - Access permission(R/W), due date, expired blocks

- **Storage “KEY AKxxx ” should be separated with source code**
- **Using personal public file storage is prohibited in TMA**
- **Commit information/data to public file storage is prohibited**

Cloud Best Practices(2)

- **Leak information of database**
  - database name + uuid, clusterID
  - Private mode, public mode→ notify to customer
- **Systems used to access to customer information/data should not downloading or copying any customer data**
- **Trusted IP are required in TMA and customer side**
- **Only authorized port services are allowed**
- **Regularly perform vulnerability scanning and access controls**

- **Allow all traffic on those ports**
- **Copying files over remote desktop**
- **Check out source code from out of office**

Quiz

- **What information is appropriate to post to public internet (e.g web blog, forum)?**
  - A. Solution document, demo of project
  - B. Project requirements, business analysis documents
  - C. Both are OK to post
  - D. Neither are OK to post
- **What information is appropriate to post to public repositories (e.g GitHub, BitBucket)?**
  - A. Source code of project
  - B. Credentials (username, password, API keys, secret keys) using in project
  - C. Both are OK to post
  - D. Neither are OK to post

Physical security

- Follow physical security procedures
- Always wear identity badges
- Ask unauthorized visitor/strangers for credentials
- Attend visitors in Reception and Meeting room only
- Escort the visitors when visiting around the office

- Bring visitors in operations area without prior permission (not follow GAA process)
- Block the automatic door closer
- Bring and use USB devices, storage devices, laptops without authorization

Clean desk & lock screen

- Lock computer screen when you leave your seat
- Store confidential documents in the locked cabinet/drawer
- Clear your desk, switch off your computer before leaving the office

- Leave your computer unlocked when unattended (lunch, meeting, training)
- Leave confidential papers, medias (CDs, tapes,…) on desk when unattended
- Leave sensitive, confidential papers on printing facilities (printer, fax, photocopier)

Passwords

- Use strong passwords/passphrases: random mixes of letters, numbers, and punctuation, 9+ characters
- Change password regularly as per policy (90 days)
- Use different passwords for different accounts

- Use passwords which reveals your personal information or words found in dictionary
- Write down or store passwords
- Share passwords with others
- Use passwords which do not match above complexity criteria

Antivirus & Patch updates

- Install official Antivirus software (McAfee) on Windows PC
- Keep Antivirus running in real-time protection mode, auto update
- Enable Auto Updates feature in OS

- Disable / uninstall Antivirus software
- Reluctant to install patch updates
- Download, install and spread illegal software, malicious software

Quiz

- **What is your best defense against virus infection?**
  - A. Don't open e-mail attachments you're not expecting
  - B. Don't surf the Internet
  - C. Don't download files from the Internet
  - D. Don't use disks to transfer data
- **Which of the following would be the best password?**
  - A. BobJones
  - B. M4krHCP&B
  - C. 12345678@X
  - D. AbcdEFgh

Internet

- Use internet services for business purposes only
- Be careful when accessing un-trusted sites
- Be careful about providing personal, sensitive or confidential information to an Internet site

- Use internet for viewing, storing or transmitting obscene or pornographic material
- Use internet for reading news or chat during office hours
- Use internet for hacking other computer systems
- Use internet to download / upload commercial software / copyrighted materials

Quiz

- **If you're not careful about your Internet browsing, which of the following can be the result**
  - A. Spyware
  - B. Viruses
  - C. Hacking
  - D. All of the above

Wifi

- Use secure wifi network (WPA2), limit use of unsecured, open wifi
- Secure your home wifi router (change default password, set string WPA2 key)
- Always use VPN client to access company resources via public Wifi

- Use company wifi for downloading big files
- Access to sensitive resources via unsecured, public Wifi
- Do not check for HTTPS indicator when accessing secure websites via public Wifi

Email

- Use official email for business purposes only
- Follow the email policy & guidelines
- If you come across any junk / spam email, do the following
  - Remove the email.
  - Inform the administrator, security team
- Use official email for personal subscription purposes
- Send unsolicited mails of any type like chain letters or email hoaxes
- Open the mail or attachment which is suspected to be virus or received from an unidentified sender
- Email addresses of co-workers

Software

- Only install and use legal, authorized software
- Return software license to Security Team when unused (e.g MS Office)

- Download, install and spread illegal software
- Use commercial software without authorization
- Use forbidden software
  - P2P file sharing
  - Tools to bypass proxy, firewall

File sharing

- Use fileserver, FTP, SVN, GIT only for business purpose

- Abuse file sharing for video, music, copyrighted materials, illegal software, etc
- Put sensitive or confidential information in public sharing folders. Exp: customer data/information (source code, test plan, feature specs,…)

Mobile computing

- Always password protect portable devices
- Run up-to-date antivirus software
- Encrypt and password protect data stored on laptops, portables devices (e.g TrueCrypt)
- Always use VPN when accessing from public internet
- Report immediately to Security Team if laptops, devices lost

- Leave laptops, devices unattended at public areas (airport, restaurant, etc)

Data backup

- Back-up critical data and software programs on PC, laptop to server
- Encrypt backup data on local harddisk

- Store original data on local harddisk without any backup
- Store backup data on 2nd harddisk of PC/laptop

Data wiping & media disposal

- Wipe harddisks, tapes, memory sticks, before recycling or re-using
- Destroy digital media before discarding
- Securely delete files which are no-longer needed (e.g Eraser)
- Use shredder to dispose sensitive, confidential papers

- Only use OS delete feature to remove data before re-using, re-cycling
- Throw sensitive, confidential papers in trash bin
- Leave confidential documents in public computers after using

Incidents & violations report

- **Proactively, timely report security incidents, violations to your Manager and Security Team within 48hours**
  - Email: security@tma.com.vn
  - Hotline: 6022

- **Discuss security incidents with external parties**
- **Attempt to interfere with, obstruct or prevent others from reporting incidents**

Contents

- What and Why Information Security?
- ISMS Introduction
- Responsibilities
- Policies and Best Practices
- **Safety Procedures**
- General Data Protection Regulation
- Security Audit
- NDA Compliance

Safety procedures

- **Building evacuation: Evacuation plan/Lab**
  - During an alarm, follow the instruction of your Evacuation Prime (one per room)
  - Evacuate calmly to the meeting point but don't hang around
  - Help people in need (injured or disabled)
- **Fire-fighting**
  - Some people in the company are trained in fire-fighting
  - These people are responsible to help contain the fire while waiting for the fire brigade, but they should not take inconsiderate risks
- **First aid**
  - Contact Admin or hospital in case of life emergency
- **Emergency contact list**

Contents

- What and Why Information Security?
- ISMS Introduction
- Responsibilities
- Policies and Best Practices
- Safety Procedures
- **General Data Protection Regulation**
- Security Audit
- NDA Compliance

General Data Protection Regulation(1)

- **General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**
- **Effective date: May 25, 2018**
- **Scope:**

  Personal data of EU residents

  Any EU or non-EU organization provides goods, services or tracking of EU residents

- **Penalty for non-compliance**

  Tier-1: 10mil EUR or 2% global revenue

  Tier-2: 20mil EUR or 4% global revenue

General Data Protection Regulation(2)

- **TMA have customers around the world**
- **TMA's customers have to comply with GDPR**
  - ✓ If they control or process personal data of living person in EU
  - ✓ One of requirements is to make sure contractors are compliant
- **TMA – as a contractor – have to comply with GDPR!**
  - ✓ Contractual obligation
  - ✓ Responsibilities are shared from Top Management to Employees

Personal Data - Examples

- Name
- Image
- Employee Personnel Number
- Address/ E-mail address
- Telephone Number
- Passport Number/ national ID
- Working hours (full or flex time)
- Driver's License Number
- Insurance Policy Number
- Education/ CV Information
- Website user ID
- Payroll data, holiday entitlement, days of absence
- Date of Birth
- IP Address leading to end-user PC
- Usage/ performance statistics

- Racial or Ethnic Origin, Political Opinions, Religious or Philosophical Beliefs
- Trade Union Memberships, Social Security, Tax or Other Similar identification numbers used by government agencies
- Personal Financial Information Including but not limited to bank account numbers, credit card numbers or debit card numbers
- Health, Criminal Record, Sexual Orientation, Genetic and Biometric Data

Special Personal data categories

Key Terms Mapping

Term	Mapping
Personal data	Information that leads to an identifiable natural person
Data subject	Clients of of customers, end-users of customers
Data processing	Broad range of activities
Data controller	TMA's customers
Data processor	TMA

Personal Data Handling Best Practices – Managers (1)

- Identify the data you process
  - Where personal data is located, processed, stored, or transmitted
- Review the process, workflow
  - Try to avoid accessing personal data in any circumstances
- Review data sharing and processing with customers
  - Contract review
  - Get written instructions from customer for personal data being processed

Personal Data Handling Best Practices – Managers (2)

- Perform a risk assessment
  - Evaluate risks and identify controls to implement
- Ensure staff are trained about data processing obligations, confidentiality, risks and security incidents identification
  - Must do, must not do, tasks and responsibilities
- Implement technical and organizational measures in team
  - Restricted access to personal data to only who need to know
  - Avoid to store personal data at TMA as much as possible
  - Keep track of personal data processing records
  - Encryption of devices (PC, laptop, mobile)
  - Immediately report security incidents

Personal Data Handling Best Practices - Engineers

- Understand data processing obligations, confidentiality
- Take customer's additional security awareness training (if any)
- Only handle data as instructed by customers
- Take Secure Coding Guidelines course
- Immediately raise about potential risks or security incidents

Contents

- What and Why Information Security?
- ISMS Introduction
- Responsibilities
- Policies and Best Practices
- Safety Procedures
- General Data Protection Regulation
- **Security Audit**
- NDA Compliance

Security audit

- **By internal team or external parties**
  - Internal audit is annually at least
  - Regular audit/spot-check of working PCs
- **Any security topic may be audited**
  - Anti-virus, clean desk, software, access control, etc
  - Observe daily operations, review documents, interview
  - How well you practice security requirements (policies, standards)
  - How well you protect confidential information
- **Violation found will be treated seriously**

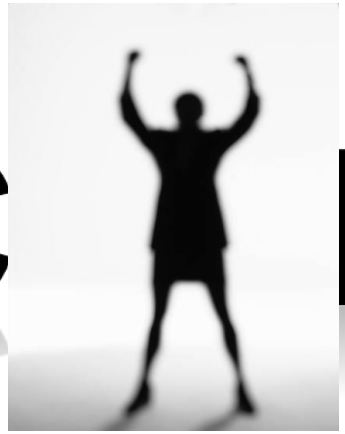
Nondisclosure Agreements

- **This Agreement shall effective all times during or subsequent to employment with TMA**
- **Data created on the corporate information systems remains the property of TMA**
- **Use for non-TMA purposes or other non-permitted purposes**
  - Exp: product information, features, source code, or name of customers, name of product, feature specs for personal purpose(personal social network, resume)

Summary

- Know your responsibilities about information security
- Follow the best practices in day-to-day work
- Stop doing bad practices that may harm information security
- Ensure confidential information is treated carefully
- Always clean desk, switch off your computer before leaving for the day
- Ensuring compliance with NDA
- Keep your self updated on information security aspects

http://intranet.tma.com.vn/qms/ISMS.html



is not complete without U

Thank you !